

- 1 -

RECORDING/REPRODUCING APPARATUS, ERROR CORRECTING
CODING METHOD AND INFORMATION RECORDING METHOD

BACKGROUND OF THE INVENTION

5 The present invention relates to an error
correcting coding method used with the recording/
reproducing apparatus.

 The Reed-Solomon code is used for the
recording/reproducing apparatus such as the magnetic
10 disk device, the magneto-optic disk device and the
compact disk device. The magnetic disk device uses the
Reed-Solomon code on the finite field $GF(2^8)$ including
 2^8 elements which is a set wherein the four rules of
arithmetic are defined (except for "division by 0")
15 mutually by the elements, where GF is an abbreviation
of Galois Field. The error correcting coding and the
error correcting process for the recording/reproducing
apparatus are performed with eight bits of the Reed-
Solomon code as one symbol providing a unit for
20 calculation.

 In the Reed-Solomon code, it is known that
the code having the maximum number t of correction
symbols can be configured by setting the number of
redundant symbols to $2t$. The length of the sector
25 providing a unit for performing each recording/
reproducing operation is 512 symbols. In view of the

fact that the length of the Reed-Solomon code that can be configured on $GF(2^8)$ is 255 ($= 2^8 - 1$) symbols or less, data are divided (interleaved) into three or more blocks and then an error correcting code is provided for each block.

One of the advantages of the Reed-Solomon code is that the symbol positions for calculation are arranged, from the most significant place of the code, as $\alpha^{n-1}, \alpha^{n-2}, \dots, \alpha^2, \alpha^1, \alpha^0$ (α : primitive root of finite field), so that the symbol position for calculation can be regularly calculated by the multiplier alone at the time of the Chien search for the error position for decoding. The Chien search is a method for searching for a solution of an equation by substituting the elements into the equation sequentially.

SUMMARY OF THE INVENTION

Consider the case in which the Reed-Solomon code on $GF(2^8)$ is used for a recording system of 512 symbols per sector. In view of the fact that the code length is not more than $2^8 - 1 = 255$ symbols and the relation holds that $512/255 > 2$, the problem is that the number of interleaves cannot be reduced below 3.

As long as the maximum number of correction symbols per sector is constant, the smaller the number of interleaves, the higher the error correcting ability of the code.

With the error correcting coding method according to this invention, an elliptic code on $GF(2^m)$ is used to configure a code longer than $2^m - 1$ and therefore the number of interleaves can be reduced.

5 For configuring the code having the maximum number t of correction symbols by the elliptic code, the number of redundant symbols is set to $2t + 1$. The number of redundant symbols for this code is $287 - 256 = 31$, and therefore the maximum number of correction
10 symbols is given as 15 ($15 \times 2 + 1 = 31$). The use of this code makes it possible to configure 512 bytes per sector in two interleaves. The principle of the error correcting coding method according to this invention will be explained below.

15 Assume that $E(C, GF(2^m))$ for the elliptic curve $C: y^2 + a_1xy + a_3y + a_0x^3 + a_2x^2 + a_4x + a_6 = 0$ on $GF(2^m)$ indicates the following set, ϵ is the number of elements of $E(C, GF(2^m))$ and $a_0, a_1, a_2, a_3, a_4, a_6$ are constants.

20
$$E(C, GF(2^m)) = \{(\alpha, \beta) \in GF(2^m)^2 \mid \beta^2 + a_1\alpha\beta + a_3\beta + a_0\alpha^3 + a_2\alpha^2 + a_4\alpha + a_6 = 0\} \dots (1)$$

$U \{o : \text{point at infinity}\}$

where if the points associated with $E(C, GF(2^m)) \setminus \{o\}$ are assigned the numbers $P^{(1)}, P^{(2)}, \dots, P^{(\epsilon-1)}$, the code
25 word of the elliptic code is defined as a column vector w satisfying $Hw = 0$ for the matrix H of equation (2).

$$H = (h_{i,j})_{\substack{1 \leq i \leq n-k, \\ 1 \leq j \leq n}}, h_{i,j} = v_{i-1}(P^{(j)}),$$

$$\left(\begin{array}{l} v_0(x, y) = 1, v_1(x, y) = x, v_2(x, y) = y, \\ v_{j+2} = v_1(x, y)v_j(x, y) \quad \text{for } j \geq 1 \end{array} \right) \quad \dots (2)$$

Especially, the code length n coincides with
 5 $\epsilon - 1$. The elliptic curve C which satisfies the
 relation $n > 2^m - 1$ can be found by total search of the
 values of the coefficient a_j .

With the definition of equation (2), however,
 the code word cannot be calculated by other than the
 10 method of solving an equation, and therefore the
 process is very complicated. The calculation can be
 facilitated by regular matrix operation of the code
 word by rewriting the equation (2) as follows.

Specifically, assume that the vector with k
 15 symbols arranged in column before coding is w_0 . When H
 satisfies equation (3), Gw_0 constitutes a code word for
 the matrix G of equation (4). As a matter of fact, the
 relation is obtained that $H(Gw_0) = M^{-1}(MH)(Gw_0) =$
 $M^{-1}((MH)G)w_0 = 0$.

20 $\exists M$: square matrix s.t. $MH = (H_1 \mid I) \quad \dots (3)$

$$G = \begin{bmatrix} I \\ H_1 \end{bmatrix} \quad \dots (4)$$

where I represents an identity matrix. If H_1 can be
 25 calculated from equation (5), the redundant symbol of

the corresponding code word Gw_0 can be calculated from w_0 .

$$Gw_0 = \begin{bmatrix} I \\ H_1 \end{bmatrix} w_0 = \begin{bmatrix} w_0 \\ H_1 w_0 \end{bmatrix} \quad \dots (5)$$

5

Equation (6) can be obtained from equation (3). As long as M is calculated and stored in advance, therefore, H_1 can be calculated. Thus, the redundant symbol of the code word Gw_0 can also be calculated from w_0 .

$$H_1 = (h_{i,j}^*)_{\substack{1 \leq i \leq n-k, \\ 1 \leq j \leq k}}, \quad h_{i,j}^* = v_{i-1}(P^{(j)}), \quad \dots (6)$$

$$\begin{pmatrix} V_0(x, y) \\ V_1(x, y) \\ \vdots \\ V_{n-k-1}(x, y) \end{pmatrix} = M \begin{pmatrix} v_0(x, y) \\ v_1(x, y) \\ \vdots \\ v_{n-k-1}(x, y) \end{pmatrix}$$

In order to give the regularity to $E(C, GF(2^m) \setminus \{0\})$, an arithmetic circuit for realizing the calculation $+_0$ as defined in equation (7) is built in and used.

$$0 +_0 P = P +_0 0 = P \quad \text{for } P \in E(C, GF(2^m)),$$

$$(x_1, y_1) +_0 (x_1, y_1 + a_1 x_1 + a_3) = 0,$$

$$(x_1, y_1) +_0 (x_2, y_2) = (x_3, y_3) \quad (x_1 \neq x_2 \text{ or } y_2 \neq y_1 + a_1 x_1 + a_3)$$

$$\left\{ \begin{array}{l} x_3 = \lambda^2 + a_1\lambda + a_2 + x_1 + x_2, \\ y_3 = (\lambda + a_1)x_3 + v - a_3, \\ \left\{ \begin{array}{l} \lambda = \frac{x_1^2 + a_4 + a_1y_1}{a_1x_1 + a_3}, \\ v = \frac{x_1^3 + a_1x_1 + a_3y_1}{a_1x_1 + a_3} \end{array} \right. \quad (x_1=x_2 \text{ and } y_2 \neq y_1 + a_1x_1 + a_3) \\ \left\{ \begin{array}{l} \lambda = \frac{x_1^3 + a_4 + a_1y_1}{a_1x_1 + a_3}, \\ v = \frac{x_1^3 + a_4x_1 + a_3y_1}{a_1x_1 + a_3} \end{array} \right. \quad (x_1 \neq x_2) \end{array} \right.$$

... (7)

5 For the element P of $E(C, GF(2^m))$, $P +_0, \dots, +_0P$ (involving Ps in the number of m) is expressed as $[m]P$.

The recording/reproducing apparatus according to this invention based on the aforementioned principle
10 is for recording in a recording medium the interleaved data with an error correcting code added thereto and reproducing the recorded data from the recording medium, the apparatus comprising an error correcting decoding circuit for generating an error correcting
15 code using an elliptic code on a finite field $GF(2^m)$ (m: positive integer).

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram showing a magnetic
20 disk apparatus using an error correcting coding method according to the present invention.

Fig. 2 is a block diagram showing a magnetic disk apparatus using an error correcting coding method based on the Reed-Solomon code.

Fig. 3 is a block diagram showing a specific example of the elliptic coding circuit of Fig. 1.

Fig. 4 is a block diagram showing a first specific example of configuration of the rational point generator of Fig. 3.

Fig. 5 is a block diagram showing a second specific example of configuration of the rational point generator of Fig. 3.

Fig. 6 is a flowchart showing the flow of the error detection/correction process of the elliptic decoding circuit of Fig. 1.

Fig. 7 is a block diagram showing an example of a syndrome calculation circuit in the elliptic decoding circuit of Fig. 1.

Fig. 8 is a flowchart showing the flow of the process in an error location polynomial calculation circuit in the elliptic decoding circuit of Fig. 7.

DESCRIPTION OF THE EMBODIMENTS

Fig. 2 is a schematic diagram showing a magnetic disk device employing an error correcting coding method based on the Reed-Solomon code. A sector of input signals 16 is converted to a sector of binary data by an interface (I/F) 14. A sector of binary data 13 is applied to a hard disk controller 9, and

segmented into three data blocks by an interleaver (ITLV-3) 11 in the hard disk controller 9. An error correction code is generated for each segmented data block by a Reed-Solomon coding circuit (RS-ENC) 6.

5 The data block 8 for which the error correcting code is generated is converted by a signal processing LSI (R/W & SPC) into an analog signal to be recorded in the magnetic disk 18 by a magnetic head. The analog signal is sent to a head 17. The signal 1
10 read from the head 17 is equalized or otherwise subjected to the signal processing such as Viterbi decoding by the signal processing LSI 3, and by being discriminated into 0 and 1 levels, converted to binary data. After conversion, the binary data 7 is applied
15 to the hard disk controller 9, and an error is detected and corrected for each decoded block of the symbol length subjected to the error correcting coding, by the Reed-Solomon decoding circuit (RS-DEC) 5.

 The three code blocks decoded are combined
20 with each other by a deinterleaver (DITLV-3), so that a sector of binary data is restored. A sector of the binary data thus restored is converted to a signal 15 for output by the I/F 14.

 This embodiment employs the Reed-Solomon
25 coding/decoding LSI circuit having the RS-DEC 5 and the RS-ENC 6 in a single chip. As an alternative, however, the encoder and the decoder may be mounted in different chips.

Fig. 1 shows a magnetic disk device using the error correcting coding method according to an embodiment of the invention. In Fig. 1, the same reference numerals as those of Fig. 2 designates
5 component elements having the same functions as the corresponding component elements in Fig. 2, respectively.

A sector of input signal 16 having 512 symbols is converted to a sector of binary data by an
10 interface (I/F) 14 for performing the analog-to-digital (A/D) conversion. A sector of the binary data 13 is applied to the hard disk controller 9, and segmented into two data blocks by the interleaver (ITLV-2) 204 included in the hard disk controller 9. The error
15 correcting coding operation is performed for each converted and segmented data block by the elliptic coding circuit 202 providing coding means. The data block 8 thus subjected to the error correcting and coding operation is converted to an analog signal 2 by
20 the signal processing LSI (R/W & SPC) 3, and applied to the head 17. The signal thus sent is recorded in the magnetic disk 18 providing a recording medium.

The signal 1 read from the magnetic disk 18 by the head 17, on the other hand, is converted to
25 binary data by the signal processing LSI 3. After conversion, the binary data 7 is applied to the disk controller 9, and an error is detected and corrected for each error corrected/coded code block of the symbol

length by the elliptic decoding circuit 5 included in the disk controller 9. The two decoded code blocks are coupled by the deinterleaver (DITLV-2) 10 and a sector of binary data is restored. A sector of the binary data 12 thus restored is converted to the output signal 15 by the I/F 14.

In the embodiment shown in Fig. 1, the elliptic coding circuit 202 and the elliptic decoding circuit 201 may be formed either on a single IC chip or on different IC chips.

Fig. 3 is a block diagram specifically showing the elliptic coding circuit (EL-ENC) 202. An input symbol train $b^{(1)}, b^{(2)}, \dots, b^{(256)}$ is input by way of an input terminal 304. A rational point generator 301 outputs a point $P^{(j)}$ at a timing when $b^{(j)}$ is input. With the point $P^{(j)}$ as an input, a vector generating circuit 302 outputs a vector $v^{(j)}$. With the point $P^{(j)}$ as an input, the matrix calculation circuit 303 outputs the vector $V^{(j)}$. With the vector $V^{(j)}$ and symbol $b^{(j)}$ as an input, a scalar multiplier 305 outputs $b^{(j)}V^{(j)}$. The output $b^{(j)}V^{(j)}$ is added to and stored in the memory 306 for storing the redundant symbols. At the same time, $b^{(j)}$ is passed through a selector 307 freely. After the processing of 256 symbols, the selector 307 selectively outputs, in descending order, the contents of the memory 306 in which the redundant symbols are stored.

In the case where the input $P^{(j)} = (\alpha_j, \beta_j, 1)$, the output of the vector generating circuit 302 is

obtained from equation (2) as $1, \alpha_j, \beta_j, \alpha_j^2, \alpha_j \beta_j, \dots$ in the descending order.

An explanation will be given of an example of preparation for the parameter calculation in decoding
5 the elliptic code $((n, k) = (287, 256))$ on $GF(2^8)$ taking the systematic coding into consideration. The code having the maximum number t of correction symbols can be configured of the elliptic code by setting the number of redundant symbols to $2t + 1$. The number of
10 redundant symbols of this code is $287 - 256 = 31$, and therefore the maximum number of correction symbols is $15(15 \times 2 + 1 = 31)$. By using this code, a sector of 512 bytes can be configured in two interleaves.

Assume that α is the primitive root of $GF(2^8)$
15 satisfying the relation $\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = 0$, and that the elliptic code configured of the elliptic curve $C_1: y^2 + \alpha^4 xy + \alpha^{25} y + x^3 + \alpha^{29} = 0$ is used.

By checking by total search whether a point on C_1 is involved or not, it is found that $\epsilon = 288$ for
20 $E(C_1, GF(2^8))$. For realizing the $+$ arithmetic circuit, assume that the input/output corresponding to o is $(0, 0, 0)$ and the input/output for the point (α_0, β_0) not o is $(\alpha_0, \beta_0, 1)$. The contents of calculation of the $+$ arithmetic circuit is configured as $(a_1, a_3, a_0, a_2, a_4,$
25 $a_6) = (\alpha^4, \alpha^{25}, 1, 0, 0, \alpha^{29})$ in equation (7).

In preparation for numbering the points associated with $E(C_1, GF(2^8))$, $[1]P, [2]P, [3]P, \dots$ are sequentially calculated at each point P of $E(C_1,$

$GF(2^8)$), and such a positive integer that gives $[m_p]P = 0$ for the first time is determined. One point where m_p assumes a maximum value is selected, and expressed as P^* . In a specific example, $\max m_p = 96$, and (α^2, α^{68}) is an example of P^* . Then, such a P^{**} is searched for that satisfies the relations $m_{p..} = \epsilon / m_p = 3$ and $P^{**} \neq [96/3]P, [2 \times 96/3]P$. In a specific example, $(\alpha^{60}, \alpha^{23})$ is an example of P^{**} .

In the process, $\{[s]P^{**} + [u]P^* | 0 \leq s \leq 2, 0 \leq u \leq 95\}$ is calculated and written out, and thus it can be checked that it coincides with $E(C_1, GF(2^8))$. Especially, a point associated with $E(C_1, GF(2^8))$ can be numbered in the form of $[s]P^{**} + [u]P^*$ ($0 \leq s \leq 2, 0 \leq u \leq 95$). $[s]P^{**} + [u]P^*$ is expressed as $P_{s,u}$, and s and u corresponding to each point on $E(C_1, GF(2^8))$ are calculated. In this way, the preparation for numbering is complete.

From the definition of s and u , the mass of (s, u) is given as a direct product group $G = Z/3Z \times Z/96Z$ of the residue class ring of integers. Also, the aforementioned numbering operation indicates that $E(C_1, GF(2^8))$ is isomorphic with $Z/3Z \times Z/96Z$ as a group.

In the description that follows, the points corresponding to the 1st, 2nd,, 287th symbols as counted from the symbol counting reference position are expressed as $P^{(1)}, P^{(2)}, \dots, P^{(287)}$, respectively.

Fig. 4 is a schematic diagram showing a rational point generator in the case where the points

associated with $E(C_1, GF(2^8))$ are numbered sequentially as $P^{(1)}, P^{(2)}, \dots, P^{(287)}$ in the order indicated in equation (8).

$$\begin{aligned} 5 \quad & P_{2,95}, P_{2,94}, \dots, P_{2,1}, P_{2,0}; P_{1,95}, P_{1,94}, \dots, \\ & P_{1,1}, P_{1,0}; P_{0,95}, P_{0,94}, \dots, P_{0,2}, P_{0,1} \quad \dots (8) \end{aligned}$$

Equation (8) is indicative of the fact that the subscript (s,u) of $P_{s,u}$ corresponds to the symbol
10 positions in lexicographic order. The counter 404 is for counting the period of descent (descending order) of subscripts from, for example, $P_{1,0}$ to $P_{0,95}$.

Fig. 5 is a schematic diagram showing an example configuration of the rational point generator
15 in the case where the points associated with $E(C_1, GF(2^8))$ are numbered as $P^{(1)}, P^{(2)}, \dots, P^{(287)}$ in the order indicated by equation (9). A part of the reference numerals designate the same component elements as the corresponding component elements in Fig. 4.

$$\begin{aligned} 20 \quad & P_{1,95}, P_{2,1}; P_{1,94}, P_{2,2}; \dots; P_{1,1}, P_{2,95}; \\ & P_{1,0}, P_{2,0}; P_{0,95}, P_{0,1}; P_{0,94}, P_{0,2}; \dots; \\ & P_{0,49}, P_{0,47}; P_{0,48} \quad \dots (9) \end{aligned}$$

25 The arithmetic circuit 502 calculates the difference of numerical value between the points $P_{s,u}$ and $P_{3-s,96-u}$ separated by semicolon in equation (9). From the manner in which P^* and P^{**} are determined and the

expression of $P_{s,u}$, the relation holds that $P_{s,u} +_o P_{3-s,96-u} = o$. From equation (7), the difference between $P_{s,u} = (\alpha_{su}, \beta_{su})$ and $P_{3-s,96-u}$ is given as $(0, a_1 \alpha_{su} + a_3, 0)$ in the input/output format of the $+_o$ arithmetic circuit.

5 Especially, the expression $P^{(j)} = (\alpha_j, \beta_j)$ satisfies the relation $\alpha_{2s+1} = \alpha_{2s+2}$.

After preparation of the foregoing process, the matrix M in the matrix calculation circuit 303, and the initial value of the memory for storing $P_{0,95}$, $P_{0,95} +_o$
 10 $P_{2,0}$ and the rational point in the rational point generator 301 indicating the symbol position are a fixed value, i.e. an encoded parameter, as far as the numbering of $P^{(1)}, P^{(2)}, \dots, P^{(287)}$ is determined. The encoder can be configured by preparing, by calculation
 15 with a calculator or the like, the matrix M from equations (3), (4) on the one hand and the initial value of the memory for storing $P_{0,95}$, $P_{0,95} +_o P_{2,0}$ and the rational point from equation (7) (taking note of the fact that the relation $P_{0,1} = P^*$, $P_{1,0} = P^{**}$ holds from
 20 the manner in which P^* and P^{**} are determined and the expression of $P_{s,u}$).

Now, an explanation will be given of an example of error detection and correction with utilizing an elliptic code. Fig. 6 shows the flow of
 25 the process for error detection and correction of the elliptic code. An error syndrome $s_0, s_1, s_2, \dots, s_{n-k-1}$ is calculated by a syndrome calculation circuit 601 for calculating the syndrome providing such a mass of check

sums as to assume zero in the absence of an error from the input. Then, the error location polynomials $f_1(P)$, $f_2(P)$ are calculated by the error location polynomial calculation circuit 602 from the error syndrome. The
5 error is located by the Chien search thereby to determine the magnitude of the error at the error location. This process corresponds to steps 603 to 609.

Fig. 7 is a schematic diagram showing the
10 syndrome calculation circuit 601. An input symbol train $z^{(1)}, z^{(2)}, \dots, z^{(287)}$ is input from an input terminal 304. The rational point generator 301 outputs a point $P^{(j)}$ at the timing of input of $z^{(j)}$. With the point $P^{(j)}$ as an input, the vector generating circuit 302 outputs
15 a vector $v^{(j)}$. With the vector $v^{(j)}$ and the symbol $z^{(j)}$ as an input, the scalar multiplier 704 outputs $z^{(j)}v^{(j)}$, which is then added to and stored in the memory 705 for storing the syndrome. After complete processing for 256 symbols, the result is output as an error syndrome
20 $s_0, s_1, s_2, \dots, s_{n-k-1}$.

Fig. 8 shows the flow of the process in the error location polynomial calculation circuit 602. This diagram shows an example of application to the elliptic code of the process called the Barlekamp-
25 Massey-Sakata algorithm (see S. Sakata, "Algebraic Geometrical Codes and the Method of Decoding Thereof", Mathematical Science, No. 421, pp. 33-40, No. 422, pp. 58-65, 1998; and S. Sakata, "A Vector Version of the

BMS Algorithm for Implementing Fast Erasure-and-Error
Decoding of One-Point AG codes", Proc. AAEECC-12,
Springer Verlag, pp. 292-310, 1997).

The calculation 606 of the error value $e^{(j)}$ in
5 Fig. 6 is carried out according to equation (10).

$$\sum_{a=0}^{2^8-2} \sum_{b=0}^{2^8-2} S_{ab} x(P^{(j)})^{-a} y(P^{(j)})^{-b} \quad \dots (10)$$

The foregoing description refers to a
10 magnetic disk device as an example. Nevertheless, the
present invention is of course applicable also to the
recording and reproduction of data in a recording
medium of other types as well as the magnetic disk
device.

15 According to this invention, the use of the
elliptic code makes it possible to reduce the number of
redundant bits as compared with the Reed-Solomon code.
Specifically, assuming that m is a positive integer and
an even number of more than 3, a code having the length
20 of $2^m + 2^{1+m/2}$ in maximum can be configured by the error
correction and coding using the elliptic code on a
finite field $GF(2^m)$. By use of the code having this
length, a sector of 512 bytes can be configured in two
interleaves.

25 In the magnetic disk device, the number of
redundant bits can be reduced as compared with the
Reed-Solomon code in which a sector of 512 bytes can be
configured in two interleaves. Assume, for example,

that the error correcting coding operation can be performed in such a manner as to correct the random error of 15 symbols in maximum. Then, the following result of comparison is obtained.

5 In the case of the Reed-Solomon code, the field on $GF(2^8)$ cannot be used but $GF(2^9)$ or larger field is required due to the limit of the code length. The maximum number t of corrected symbols is 15, and therefore in the case of the code on $GF(2^9)$, 30 (= 15 x
10 2) redundant symbols of 9 bits are added. Thus, a total of 270 (= 30 x 9) redundant bits are added.

 In the case of the elliptic code, on the other hand, the code on $GF(2^8)$ can be used. In this case, the maximum number t of corrected symbols is 15,
15 and therefore in the case of the code on $GF(2^8)$, 31 (= 15 x 2 + 1) redundant symbols of 8 bits are added. Thus, a total of 248 (= 31 x 8) redundant bits are added. As a result, it is seen that the number of
20 redundant bits of the elliptic code can surely be reduced as compared with the Reed-Solomon code.